AFRL-AFOSR-VA-TR-2022-0039

Understandable and Reusable Formal Verification for Cyber-Physical Systems

Taylor Johnson
VANDERBILT UNIVERSITY
110 21ST AVENUE S STE 937
NASHVILLE, TN, 37203-2416
US

09/03/2021
Final Technical Report

Air Force Research Laboratory
Air Force Office of Scientific Research
Arlington, Virginia 22203
Air Force Materiel Command

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
03-09-2021	Final	01 Feb 2018 - 31 Jan 2021

4. TITLE AND SUBTITLE
Understandable and Reusable Formal Verification for Cyber-Physical Systems

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-18-1-0122

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)
Taylor Johnson

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
VANDERBILT UNIVERSITY
110 21ST AVENUE S STE 937
NASHVILLE, TN 37203-2416
US

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AF Office of Scientific Research
875 N. Randolph St. Room 3112
Arlington, VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/AFOSR RTA2

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-AFOSR-VA-TR-2022-0039

12. DISTRIBUTION/AVAILABILITY STATEMENT
A Distribution Unlimited: PB Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Air Force cyber-physical systems (CPS), such as manned and unmanned aerial systems (UAS) and satellite constellations, rely on correct operation of numerous novel and legacy subcomponents over many versions during possibly decades-long lifespans.
Understanding and reusing verification results and artifacts across design iterations and abstraction layers in CPS is an unaddressed challenge that this research addresses by building on fundamental results for verification reuse in digital logic design and in purely software systems and by alleviating the state-space explosion problem. Such formal verification can ensure CPS meet their design and mission requirements and only these. Understandable and reusable verification for CPS can help address major shortcomings in current verification and validation (V&V) processes.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			TRISTAN NGUYEN
U	U	U	UU	6	**19b. TELEPHONE NUMBER** *(Include area code)* 426-7796

Understandable and Reusable Formal Verification for Cyber-Physical Systems

Final Report for Period: February 1, 2018 to January 31, 2021

Principal Investigator: Dr. Taylor T. Johnson
Institution: Vanderbilt University, Electrical Engineering and Computer Science
Award Number: FA9550-18-1-0122
Program Manager: Tristan Nguyen
Award Period: February 1, 2018 to January 31, 2021

1. Research Overview and Project Summary

Air Force cyber-physical systems (CPS), such as manned and unmanned aerial systems (UAS) and satellite constellations, rely on correct operation of numerous novel and legacy subcomponents over many versions during possibly decades-long lifespans. Understanding and reusing verification results and artifacts across design iterations and abstraction layers in CPS is an unaddressed challenge that this research addresses by building on fundamental results for verification reuse in digital logic design and in purely software systems and by alleviating the state-space explosion problem. Such formal verification can ensure CPS meet their design and mission requirements and only these. Understandable and reusable verification for CPS can help address major shortcomings in current verification and validation (V&V) processes. The research was conducted through the following objectives.

- **Objective 1:** Creating incremental model checking algorithms for hybrid automaton models of CPS, where subsequent executions of model checking algorithms reuse existing verification results, avoiding on average having to explore the entire state-space again and drastically saving computation time, particularly over design iterations.
- **Objective 2:** Developing formal abstractions for CPS by fundamentally transforming the approximations of order-reduction methods from control theory to have provable error guarantees, which can drastically alleviate the state-space explosion problem in model checking CPS.
- **Objective 3:** Designing a runtime environment middleware to interpret hybrid automata, where the middleware has been designed with provable guarantees that can preserve any properties verified using the hybrid automaton model in its actual execution in CPS.
- **Objective 4:** Evaluating the reusable formal verification methods in challenging CPS case studies with Air Force relevance, particularly distributed electric power distribution networks (microgrids) that arise in aircraft and in distributed swarm robotics systems using quadrotor drones.

In this project, progress was made in all of these objectives, as was as in new directions in autonomous CPS verification, culminating in numerous publications in journals, conference proceedings, and workshops referenced herein. Figure 1 illustrates the overall approach. HyST has also been integrated within the NNV software tool for verification of autonomous CPS that incorporate neural networks, and benefits from the advances in HyST. For Objective 1, new model checking algorithms have been developed and implemented within the HyST and NNV software tools that may incorporate prior verification results reusing the results of prior computations. For Objective 2, new automated abstractions have been implemented within the HyST and NNV software tools. For Objective 3, further integration with practical CPS design frameworks

(Simulink/Stateflow) into the HyST formal models has been performed, where formal models are transformed into models from which code generation is possible. For Objective 4, both swarm robotics and electrical microgrid case studies have been developed and investigated with the new verification methods.

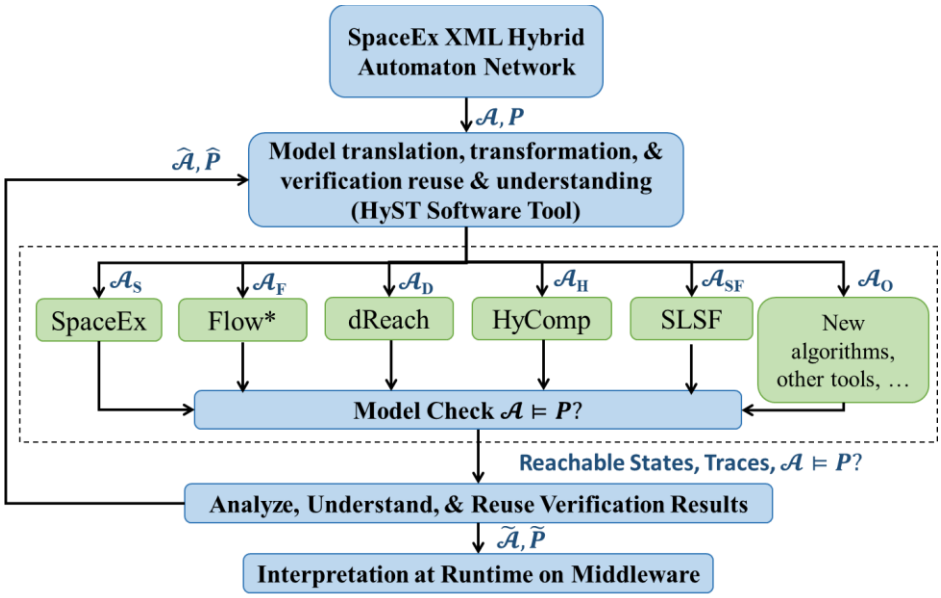

Figure 1: Overall reusable formal verification methodology for CPS, which includes developing new model checking algorithms, translating between many different verification artifacts and tools, and deploying verified models at runtime using a verified middleware to enable correct-by-construction design and implementation of CPS.

2. Accomplishments and Personnel

The following list summarizes papers, other accomplishments, software artifacts, and personnel supported in part by this research effort during this project.

2.A. Publications – Journal Articles

- Weiming Xiang, Hoang-Dung Tran, Xiaodong Yang, Taylor T. Johnson, "Reachable Set Estimation for Neural Network Control Systems: A Simulation-Guided Approach", In IEEE Transactions on Neural Networks and Learning Systems, 2020. http://www.taylortjohnson.com/research/xiang2020tnnls.pdf
- Joel A. Rosenfeld, Spencer A. Rosenfeld, Warren E. Dixon, “A mesh-free pseudospectral approach to estimating the fractional Laplacian via radial basis functions,” Journal of Computational Physics, Volume 390, 2019, Pages 306-322, http://www.taylortjohnson.com/research/rosenfeld2019jcp.pdf
- Weiming Xiang, Hoang-Dung Tran, Taylor T. Johnson, "Output Reachable Set Estimation and Verification for Multi-Layer Neural Networks", In IEEE Transactions on Neural Networks and Learning Systems (TNNLS), 2018. http://taylortjohnson.com/research/xiang2018tnnls.pdf
- Weiming Xiang, Diego Manzanas Lopez, Patrick Musau, Taylor T. Johnson, "Reachable Set Estimation and Verification for Neural Network Models of Nonlinear Dynamic Systems", In Unmanned System Technologies: Safe, Autonomous and Intelligent Vehicles, Springer, 2018, September. http://www.taylortjohnson.com/research/xiang2018ust.pdf

- Weiming Xiang, Hoang-Dung Tran, Taylor T. Johnson, "Nonconservative Lifted Convex Conditions for Stability of Discrete-Time Switched Systems under Minimum Dwell-Time Constraint", In IEEE Transactions on Automatic Control (TAC), 2018, September. http://www.taylortjohnson.com/research/xiang2018tac_b.pdf
- Omar Ali Beg, Luan Viet Nguyen, Taylor T. Johnson, Ali Davoudi, "Signal Temporal Logic-based Attack Detection in DC Microgrids", In IEEE Transactions on Smart Grids (TSG), Institute of Electrical and Electronics Engineers (IEEE), 2018, April. http://www.taylortjohnson.com/research/beg2018tsg.pdf
- J. A. Rosenfeld, R. Kamalapurkar and W. E. Dixon, "The State Following Approximation Method," in IEEE Transactions on Neural Networks and Learning Systems. doi: 10.1109/TNNLS.2018.2870040 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8509137&isnumber=6104215

2.B. Publications – Conference Proceedings Papers

- Hoang-Dung Tran, Stanley Bak, Weiming Xiang, Taylor T. Johnson, "Verification of Deep Convolutional Neural Networks Using ImageStars", In 32nd International Conference on Computer-Aided Verification (CAV), Springer, 2020, July. http://www.taylortjohnson.com/research/tran2020cav.pdf
- Hoang-Dung Tran, Xiaodong Yang, Diego Manzanas Lopez, Patrick Musau, Luan Viet Nguyen, Weiming Xiang, Stanley Bak, Taylor T. Johnson, "NNV: The Neural Network Verification Tool for Deep Neural Networks and Learning-Enabled Cyber-Physical Systems", In 32nd International Conference on Computer-Aided Verification (CAV), 2020, July. http://www.taylortjohnson.com/research/tran2020cav_tool.pdf
- Stanley Bak, Hoang-Dung Tran, Kerianne Hobbs, Taylor T. Johnson, "Improved Geometric Path Enumeration for Verifying ReLU Neural Networks", In 32nd International Conference on Computer-Aided Verification (CAV), 2020, July. http://www.taylortjohnson.com/research/bak2020cav.pdf
- Shafiul Azam Chowdhury, Sohil Lal Shrestha, Taylor T. Johnson, Christoph Csallner, "SLEMI: Equivalence Modulo Input (EMI) Based Mutation of CPS Models for Finding Compiler Bugs in Simulink", In 42nd ACM/IEEE International Conference on Software Engineering (ICSE), 2020, May. http://www.taylortjohnson.com/research/chowdhury2020icse.pdf
- Stanley Bak, Hoang-Dung Tran, Taylor T. Johnson, "Numerical Verification of Affine Systems with Up to a Billion Dimensions", In Proceedings of the 22Nd ACM International Conference on Hybrid Systems: Computation and Control, ACM, New York, NY, USA, pp. 23–32, 2019, April. http://taylortjohnson.com/research/bak2019hscc.pdf
- Hoang-Dung Tran, Luan Viet Nguyen, Nathaniel Hamilton, Weiming Xiang, Taylor T. Johnson, "Reachability Analysis for High-Index Linear Differential Algebraic Equations (DAEs)", In 17th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS'19), Springer International Publishing, 2019, August. http://www.taylortjohnson.com/research/tran2019formats.pdf
- Hoang-Dung Tran, Patrick Musau, Diego Manzanas Lopez, Xiaodong Yang, Luan Viet Nguyen, Weiming Xiang, Taylor T. Johnson, "Star-Based Reachability Analysis for Deep Neural Networks", In 23rd International Symposium on Formal Methods (FM'19),

Springer International Publishing, 2019, October. http://www.taylortjohnson.com/research/tran2019fm.pdf

- Hoang-Dung Tran, Feiyang Cei, Diego Manzanas Lopez, Taylor T. Johnson, Xenofon Koutsoukos, "Safety Verification of Cyber-Physical Systems with Reinforcement Learning Control", In ACM SIGBED International Conference on Embedded Software (EMSOFT'19), ACM, 2019, October. http://www.taylortjohnson.com/research/tran2019emsoft.pdf
- Hoang-Dung Tran, Luan Viet Nguyen, Patrick Musau, Weiming Xiang, Taylor T. Johnson, "Decentralized Real-Time Safety Verification for Distributed Cyber-Physical Systems", In Formal Techniques for Distributed Objects, Components, and Systems (FORTE'19) (Jorge A. Pérez, Nobuko Yoshida, eds.), Springer International Publishing, Cham, pp. 261–277, 2019, June. http://www.taylortjohnson.com/research/tran2019forte.pdf
- J. A. Rosenfeld, R. Kamalapurkar, B. Russo and T. T. Johnson, "Occupation Kernels and Densely Defined Liouville Operators for System Identification," 2019 IEEE 58th Conference on Decision and Control (CDC), Nice, France, 2019, pp. 6455-6460. http://www.taylortjohnson.com/research/rosenfeld2019cdc.pdf
- Weiming Xiang, Hoang-Dung Tran, Joel Rosenfeld, Taylor T. Johnson, "Reachable Set Estimation and Verification for a Class of Piecewise Linear Systems with Neural Network Controllers", In American Control Conference (ACC 2018), Special Session on Formal Methods in Controller Synthesis I, IEEE, 2018, June. http://www.taylortjohnson.com/research/xiang2018acc.pdf
- Hoang-Dung Tran, Weiming Xiang, Stanley Bak, Taylor T. Johnson, "Reachability Analysis for One Dimensional Linear Parabolic Equation", In IFAC Conference on Analysis and Design of Hybrid Systems (ADHS 2018), IFAC, 2018, July. http://www.taylortjohnson.com/research/tran2018adhs.pdf

2.C. Publications – Workshop Proceedings Papers

- Taylor T. Johnson, Diego Manzanas Lopez, Patrick Musau, Hoang-Dung Tran, Elena Botoeva, Francesco Leofante, Amir Maleki, Chelsea Sidrane, Jiameng Fan and Chao Huang, "ARCH-COMP20 Category Report: Artificial Intelligence and Neural Network Control Systems (AINNCS) for Continuous and Hybrid Systems Plants," EPiC Series in Computing 74, 7th International Workshop on Applied Verification of Continuous and Hybrid Systems (ARCH'20), Vol: 74, p 107-139, September 2020. https://mail.easychair.org/publications/download/Jvwg
- Taylor T. Johnson, "ARCH-COMP20 Repeatability Evaluation Report," EPiC Series in Computing 74, 7th International Workshop on Applied Verification of Continuous and Hybrid Systems (ARCH'20), Vol: 74, p 175-183, September 2020. https://easychair.org/publications/download/3W11
- Hoang-Dung Tran, Patrick Musau, Diego Manzanas Lopez, Xiaodong Yang, Luan Viet Nguyen, Weiming Xiang, Taylor T. Johnson, "Parallelizable Reachability Analysis Algorithms for Feed-forward Neural Networks", In Proceedings of the 7th International Workshop on Formal Methods in Software Engineering (FormaliSE'19), IEEE Press, Piscataway, NJ, USA, pp. 31–40, 2019, May. http://www.taylortjohnson.com/research/tran2019formalise.pdf
- Diego Manzanas Lopez, Patrick Musau, Hoang-Dung Tran, Souradeep Dutta, Taylor J. Carpenter, Radoslav Ivanov, Taylor T. Johnson, "ARCH-COMP19 Category Report:

Artificial Intelligence and Neural Network Control Systems (AINNCS) for Continuous and Hybrid Systems Plants", In ARCH19. 6th International Workshop on Applied Verification of Continuous and Hybrid Systems (Goran Frehse, Matthias Althoff, eds.), EasyChair, vol. 61, pp. 103–119, 2019, April. http://www.taylortjohnson.com/research/lopez2019archcomp.pdf

- Taylor T. Johnson, "ARCH-COMP19 Repeatability Evaluation Report", In ARCH19. 6th International Workshop on Applied Verification of Continuous and Hybrid Systems (Goran Frehse, Matthias Althoff, eds.), EasyChair, vol. 61, pp. 162–169, 2019, April. http://www.taylortjohnson.com/research/johnson2019arch.pdf

2.D. Oral Presentations

- Presented (virtually) “Verification and assurance tools for Cyber-physical Systems with Learning-Enabled Components,” IEEE Real Time Systems Symposium (RTSS), Application of DARPA Assured Autonomy Program Technologies to Autonomous Learning-Enabled Real-Time Systems Hot Topics Day Workshop, December 1, 2020.
- Presented (virtually) “Verifying Deep Neural Networks in Autonomous Cyber-Physical Systems,” University of Southern California, Center for Cyber-Physical Systems and the Internet of Things (CCI) and Ming Hsieh Institute for Electrical Engineering (MHI) Seminar, November 18, 2020.
- Presented “Verifying Deep Neural Networks in Autonomous Cyber-Physical Systems,” University of Memphis, Computer Science Colloquium, March 16, 2020.
- Presented “Challenges for Perception Verification in Autonomy,” at the CPS Verification & Validation: Industrial Challenges & Foundations: Safe Learning and Optimization, Carnegie Mellon University, Pittsburgh, PA, December 11, 2019.
- Invited keynote presentation, “Verification for Autonomous Cyber-Physical Systems with Machine Learning Components,” at the 6th International Workshop on Applied Verification for Continuous and Hybrid Systems (ARCH 2019), at Cyber-Physical Systems and Internet of Things (CPS-IoT) Week 2019, Montreal, Canada, April 15, 2019.
- Presented “Formal Verification: An Introduction,” DARPA seL4 Summit, September 23, 2019.
- Presented “Safety Assurance in Autonomous Cyber-Physical Systems,” University of Nebraska Lincoln, Computer Science and Engineering Colloquium, April 2, 2019.
- Presented “Safety and Security Assurance in Autonomous Cyber-Physical Systems,” University of Illinois at Urbana-Champaign, Information Trust Institute (ITI) Seminar, March 11, 2019.
- Presented “Safety Assurance in Cyber-Physical Systems built with Learning-Enabled Components,” at the CPS Verification & Validation: Industrial Challenges & Foundations: Safe Implementation of CPS, Carnegie Mellon University, Pittsburgh, PA, December 12, 2018.
- Presented “Safety and Security Assurance in Autonomous Cyber-Physical Systems with Hyperproperties & Hybrid Automata,” SimCenter Center of Excellence in Applied Computational Science and Engineering, University of Tennessee at Chattanooga, SimCenter Research Seminar, October 19, 2018.
- Presented three invited lectures on “Design-Time and Runtime Verification for Safe Autonomous Cyber-Physical Systems,” at the Summer School on Cyber-Physical Systems, Halmstad University, Halmstad, Sweden, June 11-15, 2018.

- Presented "SEC Faculty Travel Program Award Presentation: Formal Specification, Verification, & Falsification for Autonomous Cyber-Physical Systems with Hyperproperties & Hybrid Automata," at the Computer Science and Engineering Graduate Seminar (CSCE 681), Texas A&M University, College Station, TX, March 5, 2018.
- Presented paper, "Reachability Analysis for One Dimensional Linear Parabolic Equation," at the IFAC Conference on Analysis and Design of Hybrid Systems (ADHS 2018), Oxford, United Kingdom, July 12, 2018.
- Presented paper, "Benchmark: Continuous-Time Recurrent Neural Networks," at the 5th Applied Verification for Continuous and Hybrid Systems (ARCH 2018), Oxford, United Kingdom, July 13, 2018.
- Presented paper, "Benchmark: Differential Algebraic Equations (DAEs) with Varying Index," at the 5th Applied Verification for Continuous and Hybrid Systems (ARCH 2018), Oxford, United Kingdom, July 13, 2018.
- Presented paper, "Benchmark: Discrete-Space Analysis of Partial Differential Equations," at the 5th Applied Verification for Continuous and Hybrid Systems (ARCH 2018), Oxford, United Kingdom, July 13, 2018.

2.E. PhD Students Supervised and Supported by this Project

- Hoang-Dung Tran, EECS, Vanderbilt, graduated in 2020, now Assistant Professor at University of Nebraska-Lincoln
- Ayana Wild, EECS, Vanderbilt
- Xiaodong Yang, EECS Vanderbilt
- Tianshu Bao, EECS Vanderbilt

2.F. Postdoctoral Research Associates Supervised

- Weiming Xiang, EECS Vanderbilt, now Assistant Professor at Augusta University
- Joel Rosenfeld, EECS Vanderbilt, now Assistant Professor at University of South Florida

2.G. Honors and Awards Received During Period of Award

- Junior Faculty Teaching Fellow, Vanderbilt Center for Teaching, 2018.
- SEC Faculty Travel Award, 2018
- Two students supervised in our research group collaborating on this project received prestigious fellowships during the period of this project:
    - Nathaniel Hamilton, NDSEG Fellowship started in fall 2019
    - Preston Robinette, NDSEG Fellowship awarded spring 2021 to begin fall 2021
- Former postdoctoral associate Joel Rosenfeld who was supported by this project won an AFOSR YIP award in 2021.

2.H. Software Tools and Artifacts

The following software tools and artifacts were developed and improved as a part of this research effort. The tools and examples for these tools are available online.

- HyST: A Source Transformation and Translation Tool for Hybrid Automaton Models
    - http://verivital.com/hyst/
    - https://github.com/verivital/hyst
- NNV: The Neural Network Verification Tool for Deep Neural Networks and Learning-Enabled Cyber-Physical Systems
    - https://github.com/verivital/nnv